Webbinarium om

Dataläckage

när du besöker Svenska Myndigheter på nätet

Tomas Persson

Digitalist

2020-06-16

Agenda

GDPR - vad har hänt?

Massövervakning

Hur funkar webben och hur kan data läcka ut?

Webbanalys & Persondata

Hur jobbar vi på Digitalist med Webbanalys?

Vad erbjuder Digitalist för tjänster?

Frågor

Digital Entreprenör

Digital business developer

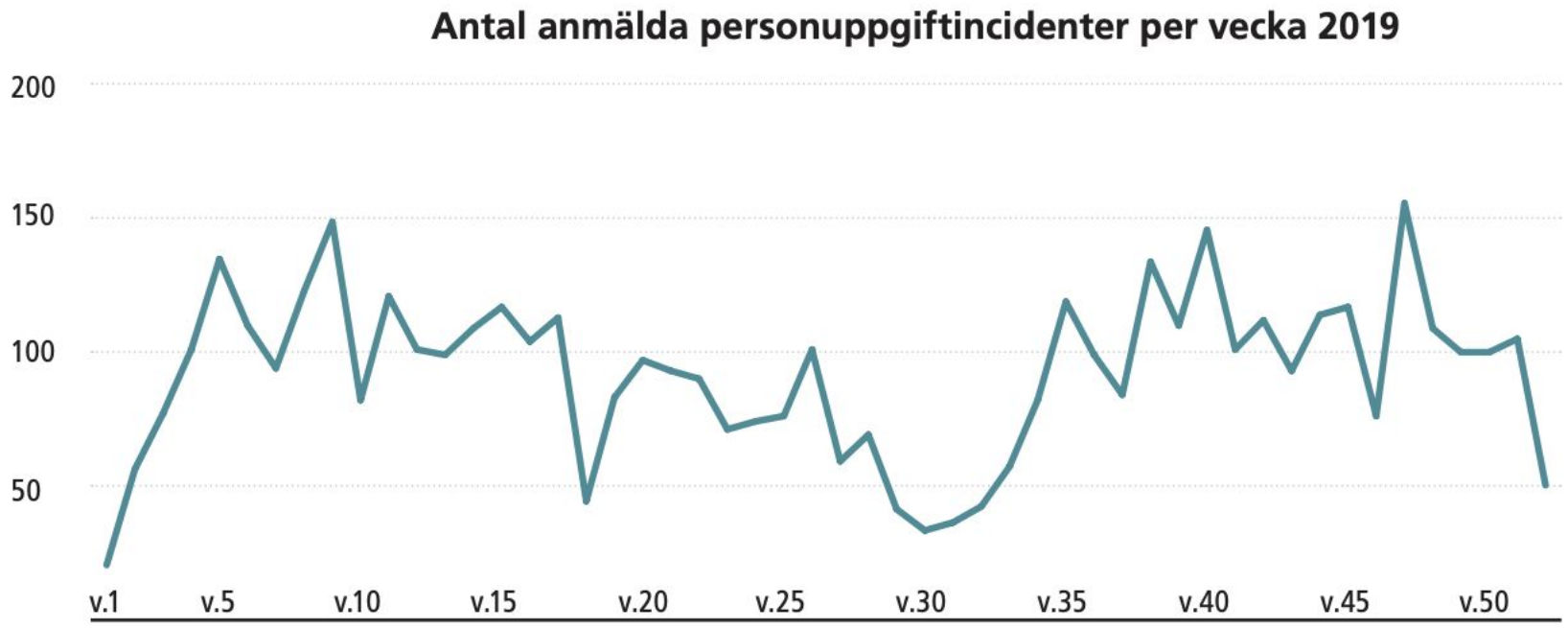
@tomper00

tomas.persson@digitalistgroup.com

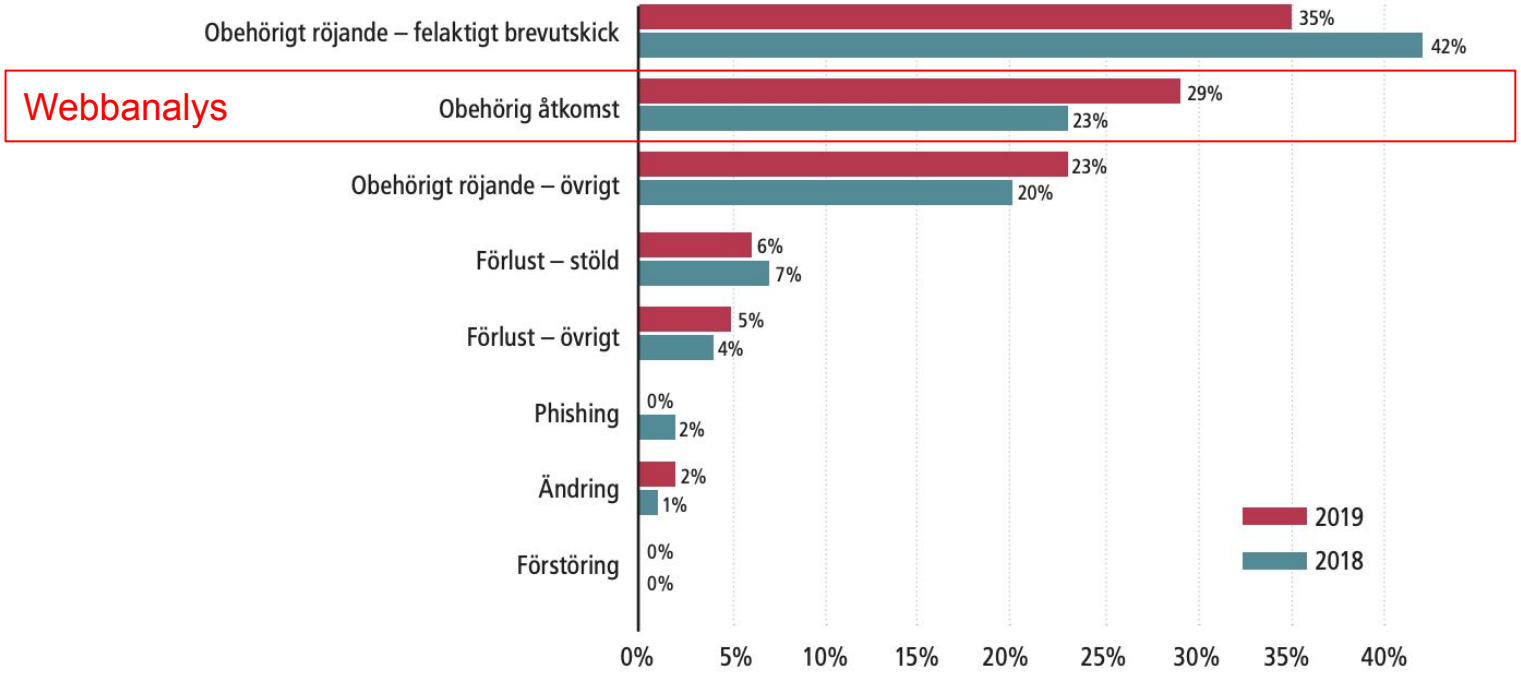
GDPR - vad har hänt egentligen?

Digitalist

Datainspektionen - 4757 anmälda incidenter 2019



Vad har hänt?


Webbanalys
Obehörigt röjande – felaktigt brevutskick
35%
42%
Obehörig åtkomst
29%
23%
Obehörigt röjande – övrigt
23%
20%
Förlust – stöld
6%
7%
Förlust – övrigt
5%
4%
Phishing
0%
2%
Ändring
2%
1%
Förstöring
0%
0%
2019
2018
0%
5%
10%
15%
20%
25%
30%
35%
40%

51% av fallen
beror på den
mänskliga
faktorn

Världen

Riggad krypteringsapparat läckte information till CIA

Washington Post

“Århundradets informationskupp”

Operationen påbörjades 1970 och pågick ända in på 2000-talet.

Dagens Nyheter: 2020-02-11

“Årtusendet informationskupp”
Edward Joseph Snowden

1978 - FISA
Foreign Intelligence Surveillance Act

9/11 2001- PSP
Presiden Surveillance Program
FISA - USA Patriot Act

2007 - TSP
Terrorist Surveillance Program

2007, 2008 FISA
2007 Protect America Act
2008 Amendment Act

2013
Edward Snowden

2018
Cloud Act
FISA renewed to 2023

Källa: https://www.eff.org/

NSA

Upstream - avlyssning

PRISM - datainsamling från företag

TREASUREMAP - realtids info från telefoner mm

William "Bill" Binney, former NSA technical director
https://youtu.be/uYg_0lmrnr4

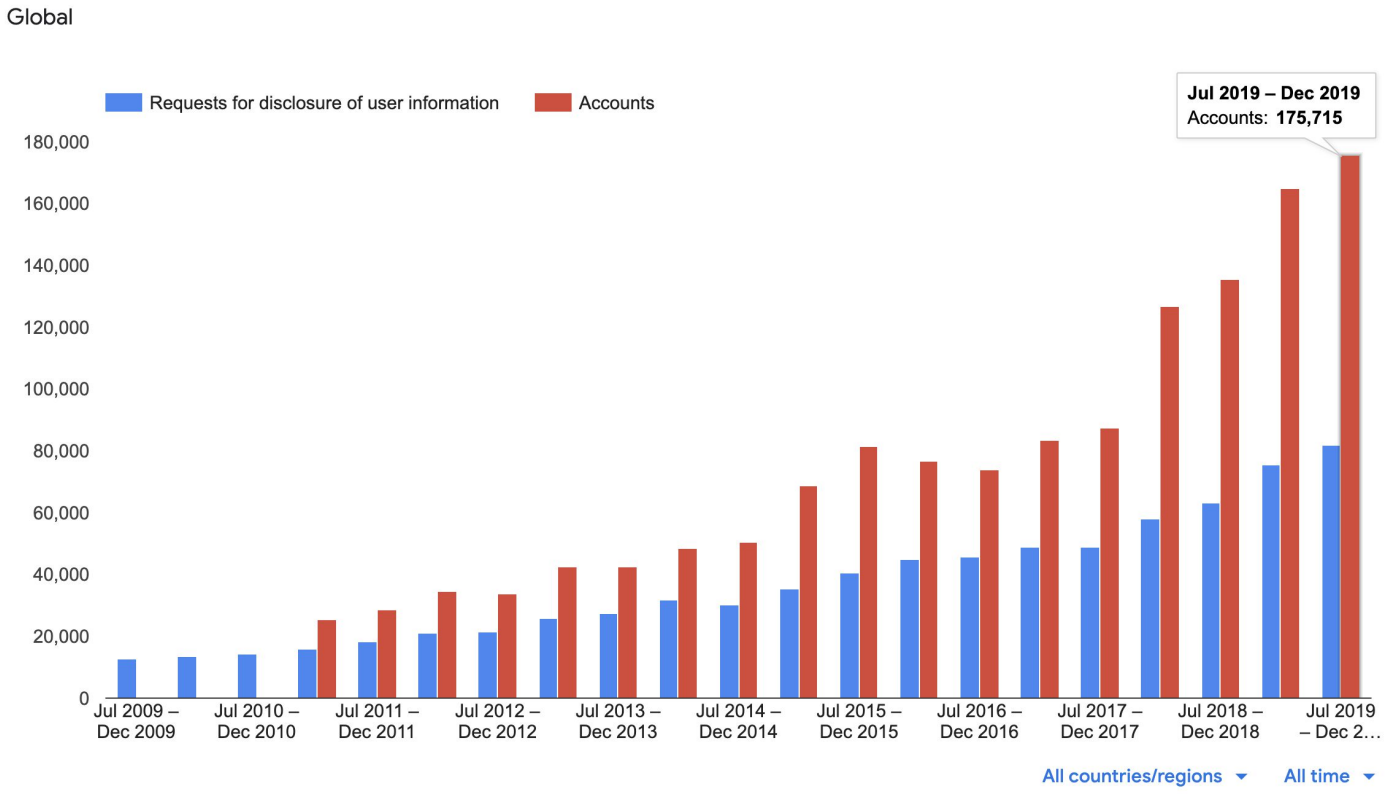
Edward Joseph Snowden

Internet trafiken i världen
Stora mängder passerar USA
NSA Samarbetar också med andra länder (tex med Svenska FRA)

Alla gillar inte detta

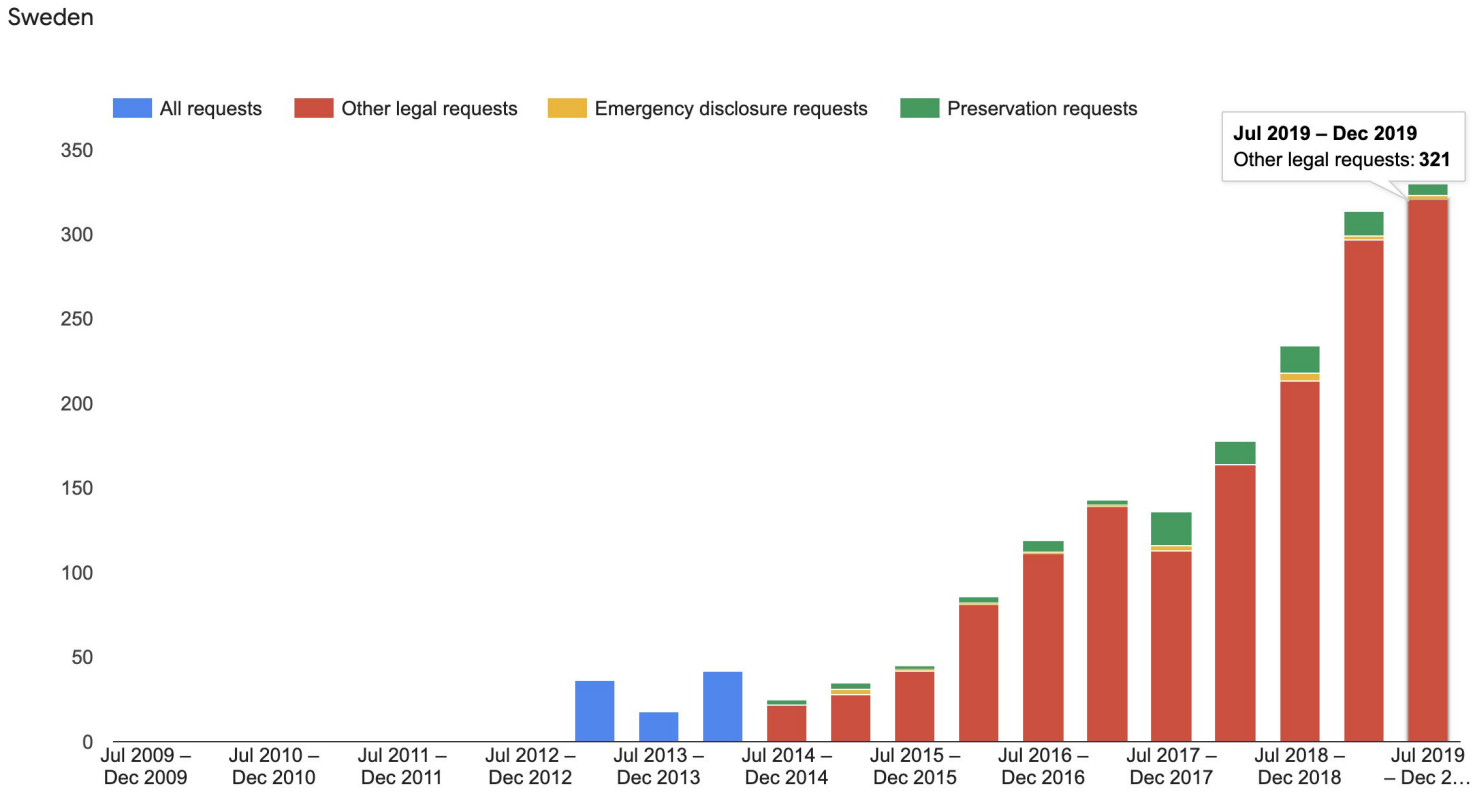
Google, Microsoft, Apple mfl kämpar emot.
+50 Amerikanska bolag redovisar därför öppet förfrågningar från myndigheterna.

Google lämnade ut Data om 175 715 användare (jul-dec 2019)



https://transparencyreport.google.com/user-data/overview?hl=en

321 st i Sverige samma period



https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:SE;time:&lu=user_requests_report_period

Sweden

All time

Government agencies, courts, and parties in civil litigation regularly ask technology and communications companies to turn over user data. In this report, we disclose information about the number and type of requests we receive from governments. We publish this information to shine light on the impact government actions have on our users and the free flow of information online.

Sammanfattning första halvåret 2019 i Sverige

Google - **321** - förfrågningar

Microsoft - **396** - förfrågningar

Apple - **104** - enheter

Facebook - **568** - konton

≈ 8 ärenden / dag i Sverige

https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report
https://www.apple.com/legal/transparency/
https://govtrequests.facebook.com/
https://transparencyreport.google.com/user-data/overview?hl=en

NSA skandaler

Mutor - Betalade RSA Security för att behålla “gamla” funktioner i sin VPN tjänst

Infiltration - Infiltrerade utvecklingen av Webbläsaren Firefox med skadlig kod.

- Blandar sig i hårdvarutvecking hos amerikanska bolag för att bygga in s.k “back doors”

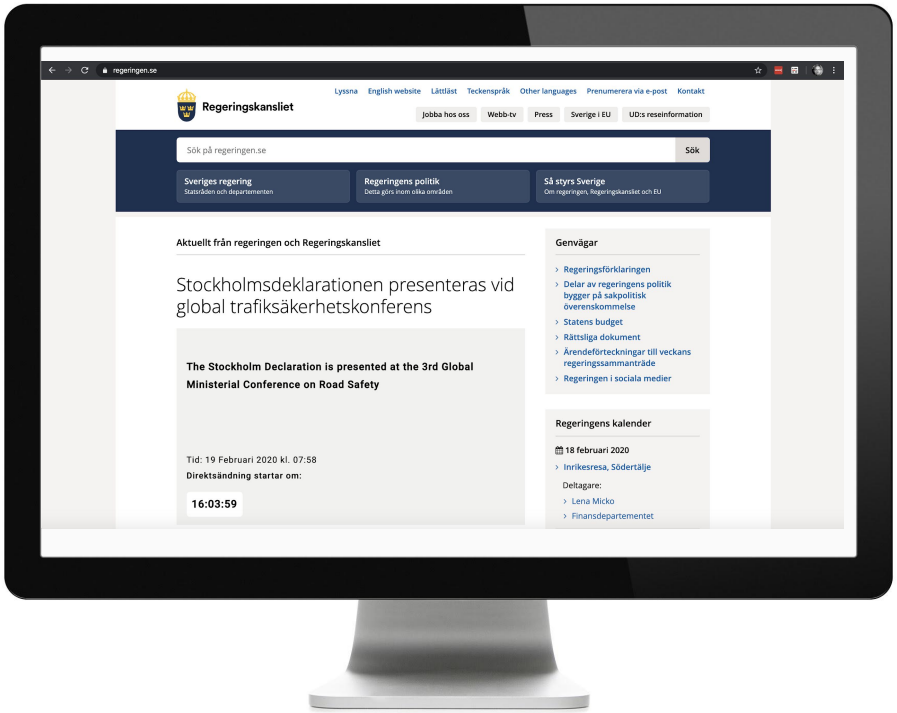
Lobbying - Investerade 250 M $ i projekt för att påverka - Public key standards

Hacking - Attackerade SWIFT för att få tillgång till banktransaktioner.

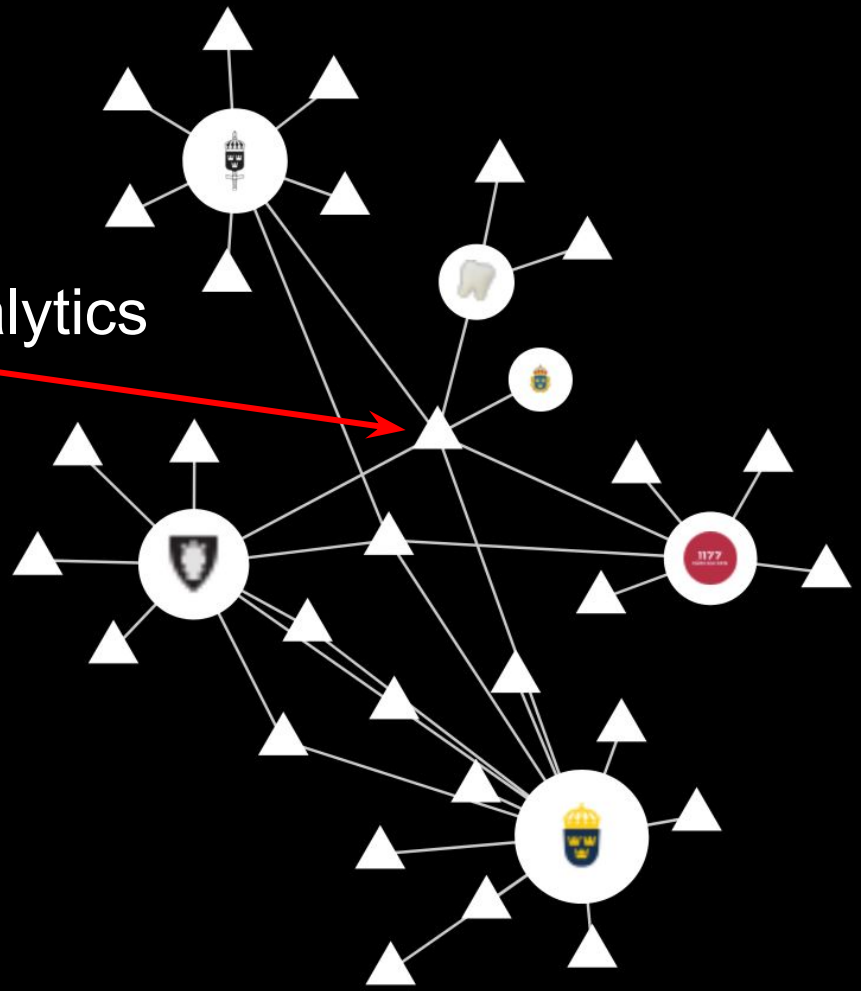
Källor:
https://www.theverge.com/2013/12/20/5231006/nsa-paid-10-million-for-a-back-door-into-rsa-encryption-according-to
https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html
https://www.infoworld.com/article/2608141/snowden--the-nsa-planted-backdoors-in-cisco-products.html
https://www.sitepronews.com/2013/10/07/nsa-infiltrated-firefox-obtain-information-tor-users-says-edward-snowden/
https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
https://www.reuters.com/article/us-usa-cyber-swift/hacker-documents-show-nsa-tools-for-breaching-global-money-transfer-system-idUSKBN17H0NX

Frågor på varför vi måste satsa på ett svenskt moln byggt på open source teknik?

Vad händer på webben vi besök på 5 webbplatser?



Google Analytics



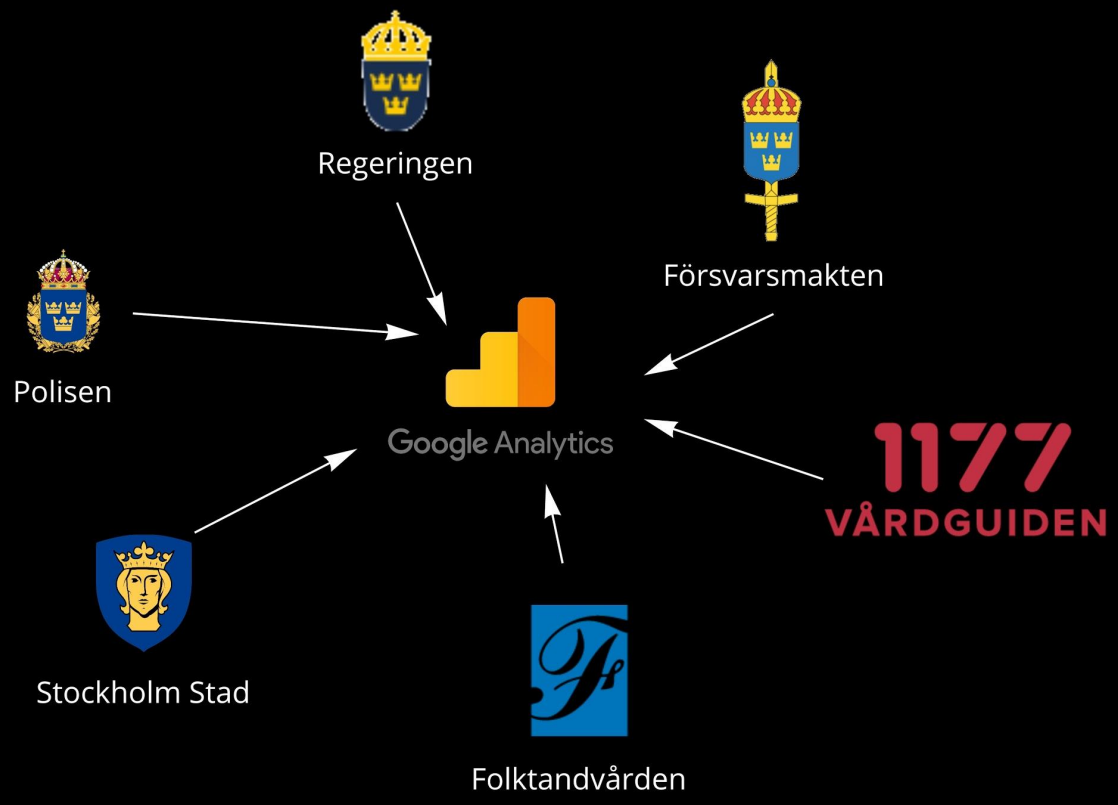
Visualisering av alla externa anrop som görs vid en sidvisning mot

1177.se
regeringen.se
polisen.se
stockholm.se
forsvarsmakten.se
folktandvården.se

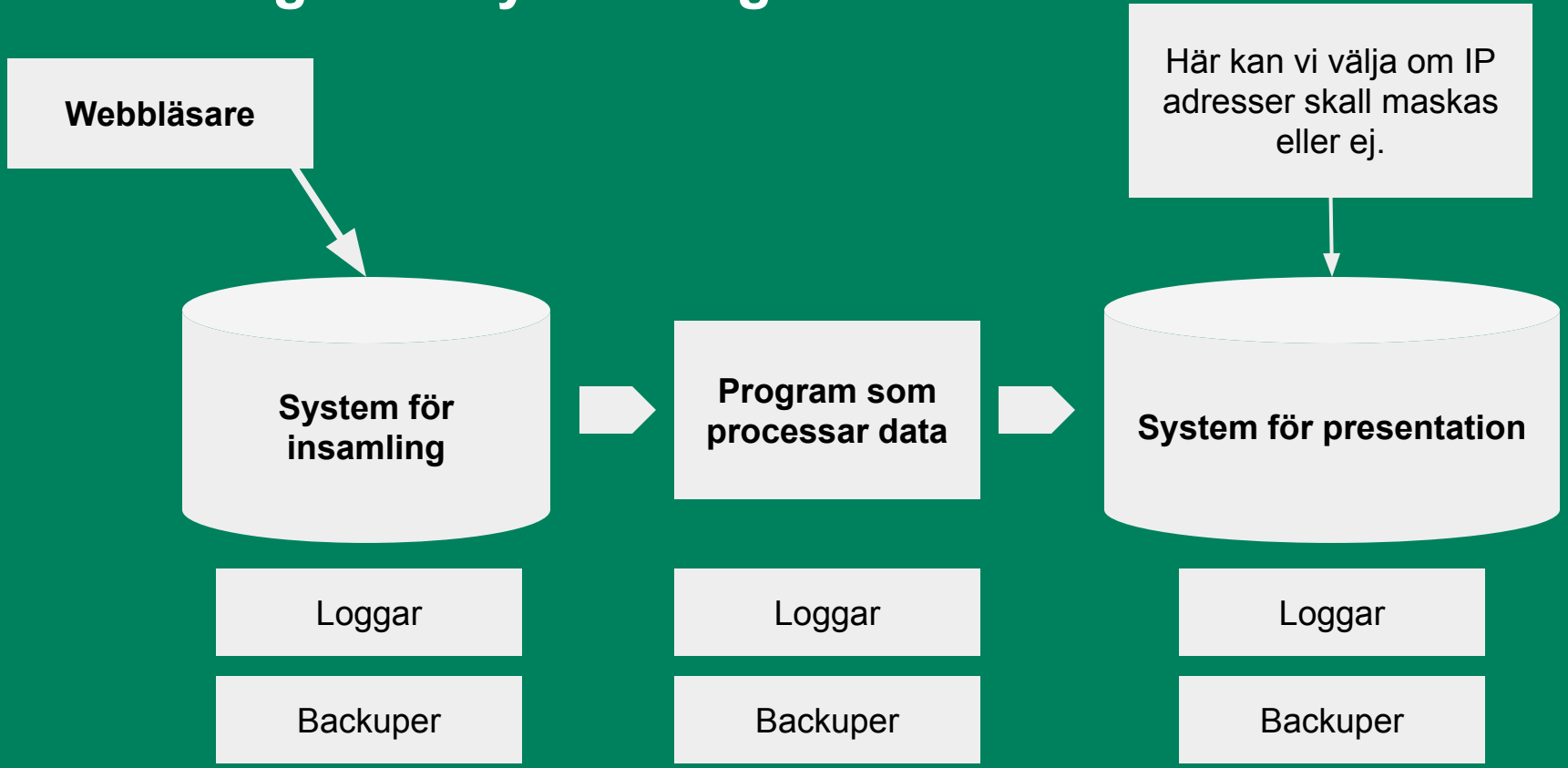
Kom ihåg - Google säljer info om våra besökare

83%

av Googles intäkter 2019
kommer från Annonsförsäljning.



Hur Google Analytics fungerar



regeringen.se/kontakt/

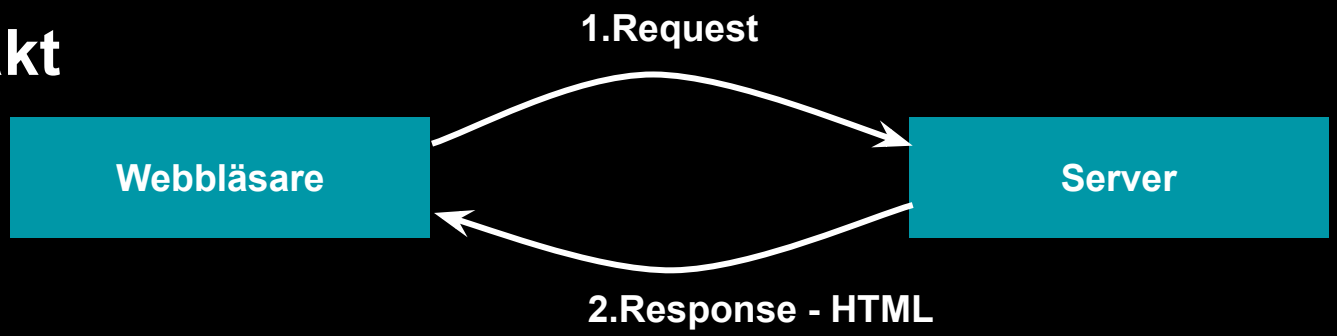
Kontakt

Kontaktuppgifter för statsråd, statssekreterare och pressekreterare hittar du på respektive statsrådssida på webbplatsen. Kontaktuppgifter till departementen finns under respektive departements sida.

Genvägar

- Kontaktuppgifter till - departementens registratorer
- Departementens besöksadresser
- Så hanteras post till regeringen och Regeringskansliet
- Regeringen och Regeringskansliet i sociala medier

/kontakt



I slutändan 33 anrop till 6 olika domäner

kontakt/	200	www.regeringen.se	document
modernizr.custom.min.30492.js	200	www.regeringen.se	script
bundle?v=p8MLSOU6gyQRqs8xcM3Li7kuA0_vXON-nMGIVNY0_p01	200	www.regeringen.se	stylesheet
GoBrain.min.js	200	play2.qbrick.com	script
logo-sv.png	200	www.regeringen.se	png
find.js	200	dl.episerver.net	script
js?v=LWrcM8g6WfrwT3dPOO3DTi0Pssi88km8O_hPGyHBx1g1	200	www.regeringen.se	script
ReadSpeaker.js?pids=embhl	200	www.regeringen.se	script
ajax-loader.gif	200	www.regeringen.se	gif
gtm.js?id=GTM-P4L58V	200	www.googletagmanager.com	script
opensans-regular-webfont.woff2	200	www.regeringen.se	font
opensans-semibold-webfont.woff2	200	www.regeringen.se	font
opensans-light-webfont.woff2	200	www.regeringen.se	font

Request

Request URL: https://dl.episerver.net/13.2.5/epi-util/find.js

Request Method: GET

Status Code: 200

Remote Address: 104.18.18.118:443

Referrer Policy: no-referrer-when-downgrade

kontakt/	www.regeringen.se
modernizr.custom.min.30492.js	www.regeringen.se
bundle?v=p8MLSOU6gyQRqs8xcM3Li7kuA0_vXON-nMGIVNY0_p01	www.regeringen.se
GoBrain.min.js	play2.qbrick.com
logo-sv.png	www.regeringen.se
find.js	dl.episerver.net
js?v=LWrcM8g6WfrwT3dPOO3DTi0Pssi88km8O_hPGyHBx1g1	www.regeringen.se
ReadSpeaker.js?pids=embhl	www.regeringen.se
ajax-loader.gif	
gtm.js?id=GTM-P4L58V	
opensans-regular-webfont.woff2	
opensans-semibold-webfont.woff2	
opensans-light-webfont.woff2	

Request headers

:authority: dl.episerver.net

:method: GET

:path: /13.2.5/epi-util/find.js

:scheme: https

accept: */*

accept-encoding: gzip, deflate, br

accept-language: sv-SE,sv;q=0.9,en-US;q=0.8,en;q=0.7

cache-control: no-cache

cookie: __cfduid=d9688888259e51a1e4d0cf79cc34596c6157

pragma: no-cache

referer: https://www.regeringen.se/kontakt/

sec-fetch-mode: no-cors

sec-fetch-site: cross-site

user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_

Den information som delas i headers gör att alla servrar vi anropar kan göra samma typ analys som vi har i Google Analytics som standard. (Pageviews med segmentering på teknologier, IP adresser mm)

8 anrop (4 domäner) når USA
google-analytics.com
google-tagmanager.com
stats.g.doubleclick.net
dl.episerver.net

I dessa anrop läcker vi (nästan) alltid

- IP adresser
- URLér

Antal anrop i Sverige
26 - regeringen.se
1 - play2.qbrick.com

Alla anrop som passerar våra gränser innebär i princip att vi inte kan leva upp till GDPR och att vi inte har en aning om vem som har tillgång till datat.

Webbanalys & Persondata

Exempel på känsliga uppgifter

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter
- biometriska uppgifter som entydigt identifierar en person

Källa: Datainspektionen.

1177 VÅRDGUIDEN | Region Stockholm | Välj region

Liv & hälsa | Barn & gravid | Olyckor & skador | Sjukdomar & besvär | Behan

Du är här: Start / Sjukdomar & besvär / Könsorgan / Könssjukdomar och sexuellt överförbara infektioner / K

Klamydia

Klamydia är en vanlig könssjukdom i Sverige. Infektionen orsakas av en bakterie och sprids framförallt genom

SVENSKA SOLDATHEMSFÖRBUNDET

Hem | Blogg | Nyheter | Kalender | Samtalsstöd | Soldathem | Familjestöd | PREP-kur

Stödtelefon

Ring: 070-570 99 91

Stödtelefon

070-570 99 91

Var går gränsen, när man kan samköra “anonyma” besök?

Polisen

Aktuellt | Tjänster och tillstånd | Utsatt för brott | Lagar och regl

Startsida / Utsatt för brott

Utsatt för brott

Hitta snabbt

Stöld av motorfordon
Stöld av mobiltelefon
Bedrägeri
Stöld eller förlust av id-handlingar...

Gör en polisanmälan

Vissa brott kan du anmäla och komplettera här på webben. För andra brott behöver du ringa eller besöka en polisstation.

IFMETALL

MEDLEM | FÖRTROENDEVALD | ARBETSGIVARE | OM OSS | KONTAKTA OSS

Startsida > Medlem > Bli medlem > Ansök direkt

Bli medlem
- Vem kan bli medlem
- Så här gör du
- Ansök direkt
- Räkna på din inkomstförsäkring

Om medlemskapet

Medlemsförmåner

Ansök direkt

Här kan du söka inträde i vårt förbund och a-kassa

Den som vill bli medlem i enbart a-kassan kan inte söka med

När du har sökt inträde kommer en bekräftelse skickas till den medlem. Får du inget mail i samband med din ansökan, kontak

När ditt inträde har behandlats får du ett välkomstbrev om ans meddelande om det.

Personlig data (PII)

(Personally identifiable information)

- IP-adresser
- E-postadresser
- Postnummer
- Personnummer
- Kreditkortsnummer
- Namn
- Telefonnummer
- osv.

Personliga data

!

men personlig data är också.

Data som i kombination med annan data kan identifiera en person

Ort: Hyltingeö
Enhet: Samsung galaxy S8
Kön: Man
Ålder: +60
Intresse: Politik
Gissa personen

Vi måste därför ha rutiner som utgår ifrån att vi kommer att hitta PII.

PII incident
Exempel på Handlingsplan

1. Bedöm allvarlighetsgrad
2. Förhindra ytterligare insamling
3. Besluta om eventuell rapport till datainspektionen (inom 72 h)
4. Rensa data
5. Dokumentera incidenten
6. Informera drabbade?
7. Retrospektiv

Hur jobbar Digitalist med detta?

matomo

Open Source alternative to Google Analytics

Vi hjälper bla Skatteverket, Arbetsförmedlingen, Trygghetsrådet, Vattenfall och Lärarförbundet med Matomo

Säkrad webbanalys med Matomo

- System & Data på rätt fysisk plats (baserat på Open Source)
- Personbiträdesavtal med alla parter som kan ha access till datat
- Koll på var alla loggar och backuper sparas och hur länge. (max 30 dagar)
- Schemalagd rensning av insamlat data (1-2 år normalt)
- Stöd för medgivande vid spårning

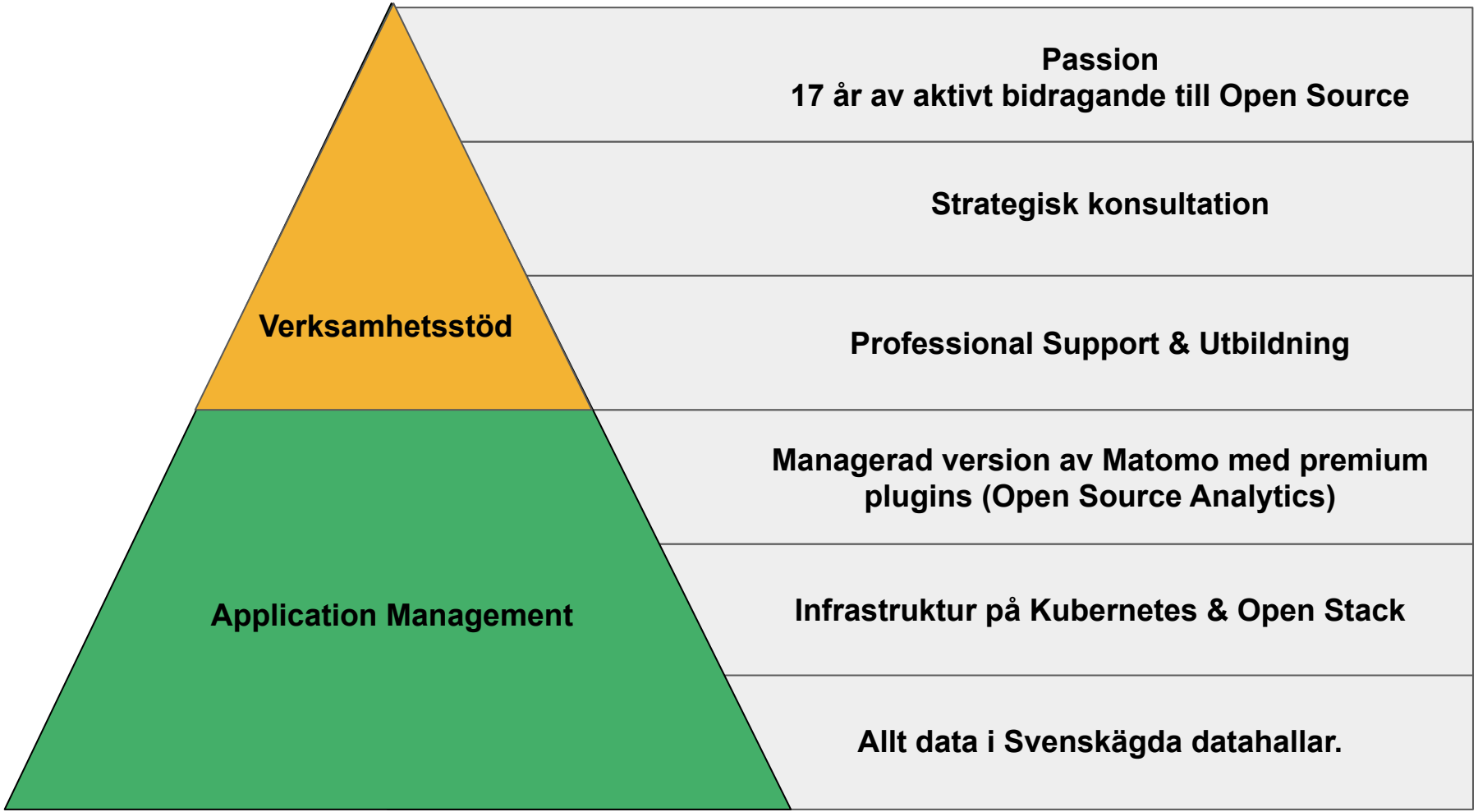
Våra rutiner kring Persondata

- Övervakning av data vi samlar in - identifiera PII - Larm
- Standardiserade mätskript (minska mänskliga fel)
- Rutiner, kompetens och verktyg för att kunna hantera om (när) vi identifierar PII.
- Utbildning / stöd till utvecklare

Kompetens att bygga och förvalta webb

- Grundläggande Kunskap om HTTP(S), certifikat, servrar etc
- Löpande uppdatera och övervaka sin kod (inget är statiskt på webben)
- Kunskaper om vad och hur data kan samlas in

Vad erbjuder Digitalist?


Verksamhetsstöd
Application Management
Passion
17 år av aktivt bidragande till Open Source
Strategisk konsultation
Professional Support & Utbildning
Managerad version av Matomo med premium plugins (Open Source Analytics)
Infrastruktur på Kubernetes & Open Stack
Allt data i Svenskägda datahallar.

VISIONEN

Att erbjuda fler säkra tjänster mot Produktägare av digitala tjänster på Open Source.

Dashboards, Enkätverktyg, Marketing automation, Personalisering, Machine learning etc.

Utvärdera Matomo med premium plugins gratis!
Maila till
tomas.persson@digitalistgroup.com

Frågestund